DZ BANK

REQUIREMENTS FOR THE BCM OF THE CONTRACTOR

1. RESPONSIBILITY OF THE MANAGEMENT BOARD LEVEL

1.1. The Management Board level bears overall responsibility for Business Continuity Management (BCM) and must define and document its objectives and scope. This documentation must be binding and ensure that all decisions can be clearly understood in retrospect. The BCM process must additionally be initiated, managed and controlled.

1.2. The Management Board level must ensure that the BCM system is reviewed and evaluated regularly to confirm that it is up-to-date and appropriate and that corrective measures are initiated where applicable. If the Management Board delegates the operational implementation of these tasks to others, they must be implemented by a central role (e.g. Business Continuity Manager).

1.3. The Management Board level must be kept informed about the state of BCM at least once a year, for example, through status reports (on BCM activities and results, risks).

1.4. The Management Board level must ensure that sufficient financial, technical and staff resources are made available for the aspired BCM objectives and that the resources are reviewed once a year and on an ad hoc basis to ensure that they meet current requirements and are amended where applicable.

2. REQUIREMENTS, SCOPE OF VALIDITY AND OBJECTIVES

2.1. The services agreed with DZ BANK must be covered by the BCM system.

2.2. The methodological orientation of the process model for the establishment and continual operation of the BCM must be set down in a policy (e.g. orientation towards the BSI standard on BCM or ISO 22301). The policy must be reviewed at regular intervals (at least every four years) as well as in the event of significant changes in the underlying conditions, business objectives, tasks or strategies to determine whether amendments are required and to implement these if they are needed.

3. TASKS, COMPETENCIES AND RESPONSIBILITIES

3.1. The roles of BCM and the respective tasks, duties and competencies of these roles must be adequately defined and documented to reflect the prevailing circumstances. This includes the formal appointment of a Business Continuity Manager who is responsible for the maintenance and further development of the BCM.

3.2. The BCM organisational structure must be reviewed annually to verify its adequacy. Changes must be taken into account (e.g. changes in size, and the locations and organisational units that it covers).

4. INTERFACES, COMMITTEES AND COMMUNICATION

4.1. All BCM policies, processes, and responsibilities must be regularly and, when necessary, ad-hoc coordinated and aligned with related management disciplines (e.g., information security) to ensure compliance with security objectives and to support an overall security strategy.

5. TRAINING AND AWARENESS-RAISING

5.1. Employees who are assigned BCM tasks and responsibilities must receive training in accordance with their required competences and must be informed annually about their role-specific tasks and changes in BCM.

5.2. All employees must receive awareness training on the topic of BCM on a regular basis (at least every two years).

5.3. Training and awareness-raising measures must be documented in a BCM training and awareness program, and the implemented measures must be documented (e.g. in the form of participant lists, certificates, confirmations of attendance).

6. BUSINESS IMPACT ANALYSIS (BIA) – METHODOLOGY

6.1. A systematic analysis of the effects of an outage of each business processes / activity or each activity per organisational unit must be conducted annually as well as on an ad hoc basis (Business Impact Analysis). This analysis must have a time reference (e.g. expected damage due to an out-age of business processes / activities within the categories <4 hours, <1 day ... <5 days). Existing results (e.g. BIA results from the previous year) can serve as a basis and must be updated accordingly.

6.2. The assessment of the damage must not only take economic and financial repercussions into account but also potential loss of reputation and legal consequences.

6.3. The BIA to be conducted must take into account at least the resources: facilities, staff, IT and service providers.

6.4. The analysis of the effects of an of a business-process / business-activity outage must identify the following information:

- Maximum Tolerable Period of Disruption (MTPD)
- Recovery Time Objective (RTO)

6.5. Mutual dependencies of the business processes / activities (process chains) as well as the resources required for emergency operations, i.e. time-critical resources (especially workplaces, IT, staff roles / functions, third party arrangements) must be determined, documented and – in the event of mutual dependencies – inherited.

6.6. The methodology and procedure for the BIA must be documented in a methodological and pro-cess description which ensures that they remain comprehensible ex post.

6.7. It must be ensured that business processes / activities which are indispensable for overcoming IT- / IT security-related emergencies and crises are assigned the highest possible availability requirements.

7. RISK ANALYSIS

7.1. A systematic assessment of potential risks that could lead to a failure of business processes / activities or resources must be conducted annually and on an ad hoc basis. The methodology to be employed for conducting the Risk Analysis must be documented. New risks must be analysed in accordance with the above-mentioned methodology; risks that have already been identified and assessed must be inspected for changes. Existing results (e.g. the results of the previous year's Risk Analysis) can serve as a basis and must be updated accordingly.

7.2. The risk analysis is designed in such a way that a catalogue of risks and scenarios is considered, which is based on common standards and currently valid regulatory requirements.

7.3. The results of the Risk Analysis must be documented and made available to the Management Board level for information purposes (where applicable, as part of an overall risk status).

8. BCM STRATEGIES AND RISK HANDLING

8.1. Based on the results of the Business Impact Analysis and Risk Analysis, it is necessary to develop and update suitable business continuity strategies which allow the critical business processes / activities to be restarted in emergency operations within the required time, to maintain emergency operations and to restore and return to regular operations.

8.2. At least for the time-critical resources, a plan must be developed for handling each risk which, in accordance with the Risk Analysis, is identified as requiring action to handle the risk and for which no risk toleration has been documented, for reducing the impact, probability of occurrence and downtime.

8.3. The risk owner must conclusively confirm a toleration of the residual risk and document this.

9. BUSINESS CONTINUITY DOCUMENTATION

9.1. Documentation (Business Continuity Plan / BCP) must be developed which is activated in the event of a significant interruption of business operations and which describes the activities need-ed to achieve and maintain the specified emergency operations based on the availability requirements of the Business Impact Analysis.

9.2. The documentation (BCP) must contain details of the preparation for emergency operations as well as the return from emergency operations for the scenarios staff shortage (e.g. due to loss of key personnel, pandemic situations), facility failure (e.g. due to natural disasters, power outage), IT outage (e.g. due to cyber-attack, substantial failure of IT assets or the communication infra-structure) and failure of service providers (e.g. due to quality of service deteriorates to an unacceptable level or fails, strike).

9.3. It must be ensured that all reactive emergency documents undergo yearly and / or ad hoc re-views to ensure that they are complete and up to date.

10. IT RESTART AND DISASTER RECOVERY PLANNING

10.1. It must be ensured that documented IT Restart and Disaster Recovery plans are available for all BCM-relevant IT assets which ensure that the resource can be restarted from an IT perspective within the Recovery Time Objective (RTO) specified in the BIA.

10.2. Once a year, the results of the BIA must be compared with the latest status of the IT Restart plan (target / actual comparison between RTO / RPO from the BIA and the implementation status). If any gaps are identified, it must be ensured that improvement measures are initiated.

10.3. The IT Restart plan must document the sequence in which IT assets are to be restarted, including the expected duration of the entire restart.

11. STRUCTURAL / TECHNICAL DATA CENTRE SECURITY

11.1. A Risk Analysis must be prepared for every data centre in which BCM -relevant IT assets are operated, showing the vulnerabilities and threats which are to be expected at the location concerned. In particular, environmental risks (e.g. flooding, earthquakes) and potential neighbourhood risks must be reviewed.

11.2. The physical distance between the data centres must be checked and ensured for their compliance with legal / regulatory or internal guidelines. The Risk Analysis and risk situation must be taken into account in doing so.

12. DATA BACKUPS

12.1. It must be ensured that a documented data backup concept is in place which regulates the Recovery Point Objective (RPO) of all BCM-relevant IT assets and the data associated with them. These guidelines will also apply to offsite storage.

12.2. Data backup media must be held in storage at a location which is physically separate from that of the IT systems that originally saved the data.

12.3. It must be ensured that data backup media are stored redundantly at a remote location (at least in a separate fire compartment). The adequacy of the distance must be determined taking into account the individual risk and data backup situation.

12.4. It must be ensured that the data backups can be accessed sufficiently quickly when they are needed.

12.5. Data backups must be tested once a year to ensure that they are readable. The results must be recorded.

13. BUSINESS CONTINUITY AND CRISIS MANAGEMENT ORGANISATION STRUCTURE

13.1. It must be ensured that all Business Continuity- and Crisis Management activities are controlled, coordinated and monitored centrally and that responsibilities for strategic-level decision-making during an emergency or crisis are defined and documented (e.g. by a business continuity response team or crisis management team).

13.2. It must be ensured that organisational regulations ensure a planned and organised procedure during the handling of an emergency or crisis and that the requirements of business operations (in particular availability requirements in accordance with the Business Impact Analysis) are taken into account.

14. NOTIFICATION, ALERT AND ESCALATION

14.1. Rules on reporting, alerting and escalating damaging events must be established and documented; these should cover the following aspects:

- definition of threshold values (transition from an incident to an emergency),
- qualification of the event (definition of the parties to be notified, decision on when an incident is qualified as an emergency or crisis),
- mobilisation of the reactive BCM or Crisis Management organisation structure and
- communication channels to be used.

15. BUSINESS CONTINUITY EXERCISES / TESTS

15.1. The planning of exercises / tests must be documented in an exercise / test program (e.g. annual plan). This must take into account: within a period no more than three years, all business processes / activities classified as BCM -relevant and time-critical as well as all time-critical re-sources must be covered in the framework of tests and exercises. BCM tests involving IT assets must take into account the infrastructure as well as the components of an application cluster.

15.2. When planning the exercise and test program, at least the scenarios that could lead to serious emergencies or crises according to the probability of occurrence based on the hazard situation or risk analysis must be taken into account.

15.3. For time-critical IT assets (availability requirement e.g. <4 hours or <1 day), it is mandatory to conduct Restart tests once a year. In addition, for highly time-critical IT assets (availability requirement e.g. <4 hours), Disaster Recovery tests consisting of a system recovery and data recovery must be performed every three years.

15.4. All exercise / test results must be recorded.

15.5. Aborted or cancelled exercises / tests as well as exercises / tests with serious findings must be repeated or planned anew. This must be documented accordingly in the exercise / test pro-gramme.

15.6. All exercises / tests must be investigated for possible follow-up measures in the course of the review process (see chapter “Reporting and Review”).

15.7. A Business Continuity response / Crisis Management team exercise which includes the roles / functions of the BCM / Crisis Management organisation structure must conducted within a maximum period of three years.

16. OUTSOURCING / THIRD PARTY ARRANGEMENTS

16.1. It must be ensured that the Service Level Agreements (SLA) between DZ BANK and the contractor are not adversely affected by the sub-contracting to further parties.

16.2. Externally operated BCM-relevant services (sub-contracting) must comply with the DZ BANK SLAs (e.g. <4 hours for highly time-critical services or <1 day for time-critical services).

16.3. Synchronized BCPs must be prepared for all third party and BCM-relevant service provider agreements and be reviewed once a year to ensure that they are up to date.

16.4. Sub-Contractors must undertake to provide customer reports, e.g. within the scope of ISAE3402 or PS951 reports, in order to document compliance with the requirements in the event of sub-contracting.

17. AUDIT AND TRACKING OF MEASURES

17.1. The roles responsible for BCM must define and conduct systematic audits and performance evaluations to ensure that the BCM methodologies and policies are complied with.

17.2. Audits and performance evaluations and their respective control criteria must be specified based on the defined BCM processes and be documented in a manner which ensures that they remain comprehensible ex post. The results of audits and performance evaluations must also be documented and kept in a manner which ensures that they remain comprehensible ex post.

17.3. It must be ensured that findings from arisen emergencies lead to a review and, where applicable, an amendment of the existing measures and organisational and technical BCP documents.

17.4. Any problems identified during an audit and performance evaluation must be eliminated as quickly as possible. The necessary remedial measures must be devised by persons responsible in BCM, documented (who does what by when) and verified for implementation.

17.5. If they have not been implemented in due time, the matter must be escalated with Management Board level involvement.